HOLISTICA Vol 14, Issue 1, 2023, pp.110-132 DOI:10.2478/hjbpa-2023-0007

HUMAN ERROR - A CRITICAL CONTRIBUTING FACTOR TO THE RISE IN DATA BREACHES: A CASE STUDY OF HIGHER EDUCATION

Katherine AMORESANO[1]
Benjamin YANKSON[1]*

Received: December 2022 | Accepted: April 2023 | Published: June 2023
Please cite this paper as: Amoresano, K., Yankson, B. (2023) Human error - A critical contributing factor to the rise in data breaches: a case study of higher education, *Holistica Journal of Business and Public Administration*, Vol. 14, Iss. 1, pp.110-132

Abstract

With increasing technical safeguards to protect information systems, Human error continues to be a critical factor contributing to the rise in information systems attacks and data breaches. Inadequate or unenforceable Cybersecurity policies or training can open doors for adversaries to circumvent technical safeguards and paint a picture of a growing cybersecurity problem. The problem investigated in this work assesses if organizations adequately invest in resources to provide industry-aligned cybersecurity education, training, and awareness that can minimize human error leading to cyber-attacks. This work aims to investigate breaches attributed to human errors and compare cybersecurity policies, education, training, and awareness programs in three different schools in New York State. The work focused on user awareness and vulnerable behaviours, effective training for users, and investigating start-of-the-art approaches to gauge or evaluate the organization's cybersecurity stance when compared to industry frameworks like the NIST framework. A Triangulation research approach including quantitative, qualitative, and descriptive methods are adopted for this work. Instruments for data collection include a survey, literature review, qualitative analysis to identify research gaps, and assessments of the questionnaires. This work demonstrates that formulated enforced cybersecurity policies coupled with targeted security education, training, and awareness are instrumental to decreasing user errors, thereby reducing the probability of a cyber-attack.

Keywords: Human Error; Security; Policies; Training; Attacks

1. Introduction

The problem of Human error in Cybersecurity refers to a variety of mistakes made by users rather than the failure of the computer, technology, or machine being used (Webster, 2020). The mistakes that lead to successful cyberattacks are more commonly

[1] *HackIoT Lab, University at Albany, State University of New York. 1400 Washington Ave, Albany, NY 12222. USA, byankson@albany.edu.*
** Corresponding author*

from human errors than problems with the technology itself (Nobles, 2018). Before the 21st century, the use of computers by everyday users for work was not as prominent as today. Presently, an increasing number of users use computers for day-to-day activities at work; therefore, providing more opportunities for attackers to leverage dire errors to launch massive cyberattacks on business systems or critical infrastructure, costing the organization millions of dollars. Cyber-attacks are currently happening at an increasing rate in both the private and public sectors. These attacks impact millions of individuals who use information systems daily. The attacks can come from many sources, such as "nation-states, criminal syndicates, cybervandals, intruders hired by unscrupulous competitors, and disgruntled insiders (Winnefeld et al., 2015). The average annual cost of data breaches caused by human error is $3.36 million ("Cost of a Data Breach Report," 2019). While the most common cause for security breaches is malicious actors, human error is one of the top three root causes and must be addressed accordingly (Keierleber, 2022). A 2021 IBM report (IBM, 2022) demonstrated that the United States is the leader in recording some of the most expensive data breaches globally. On average, the worldwide expense associated with a data breach has surpassed $4 million, more expensive than the 3.6 million predicted by Ponenom Institutes in their 2020 report (IBM, 2019) (Barati, et.al, 2022). To put this into context, from 2005 to 2019, a report from the Privacy Rights Clearinghouse (PRC) depicted approximately 9,015 successful attacks, which amount to 11,690,762,146 breached records (Privacy Rights Clearinghouse, 2021). Such attacks containing data breaches demonstrate that attackers continuously adapt and devise new unique techniques to exploit or evade existing security controls to gain access to sensitive and critical information.

A primary issue businesses, especially higher educational institutions, suffer from this problem face today is the lack of widespread knowledge on providing adequate cybersecurity policies, training, and awareness to users on how to protect information systems. In recent years, human error in computer security has been the primary reason for breaches, as opposed to having problems with the hardware or software (Ahola, 2022). Many studies (IBM, 2022), (Nobles, 2018), (Ahola, 2022). have shown that the current cybersecurity policies, training, and awareness for employees within the public sector, especially the higher education sector, are inadequate or not accessible to users causing frequent human errors (Ahola, 2022) . For example, in a 2014 IBM study, human error resulted in over 95% of all information system security breaches (IBM, 2014). A follow-up study by IBM in 2019 examined the top three root causes (malicious or criminal attack, system glitch, and human error), which shows that human error accounted for 24% of them (IBM, 2019).

Further, as per the 2022 Checkpoint (Marcelino, 2022) report, there was an approximately 44% rise in cyberattacks within the education sector as compared to 2021, which reported 2297 weekly average cyber-attacks against educational institutions. Such attack growth can be supported by recent FBI and CISA advisory of ransomware threats "disproportionately targeting the education sector" (Keierleber, 2022). Further other works, such as a 2021 survey conducted by Sophos, a global

cybersecurity leader (D'agostino), consisting of 5,600 Information Technology(I.T.) professionals with approximately 410 participants from higher education and cutting multiple countries, showed a surge in cyberattacks such as Ransomware. The result demonstrates that these attacks have high costs to the impacted Institution. The report further stated a higher ransomware attack success rate in higher education compared to other domains, such as healthcare. For example, the report found that almost 74% of ransomware attacks succeed. The success rate is 61% for healthcare, 68% for business, and 57 % for financial services (Keierleber, 2022) .

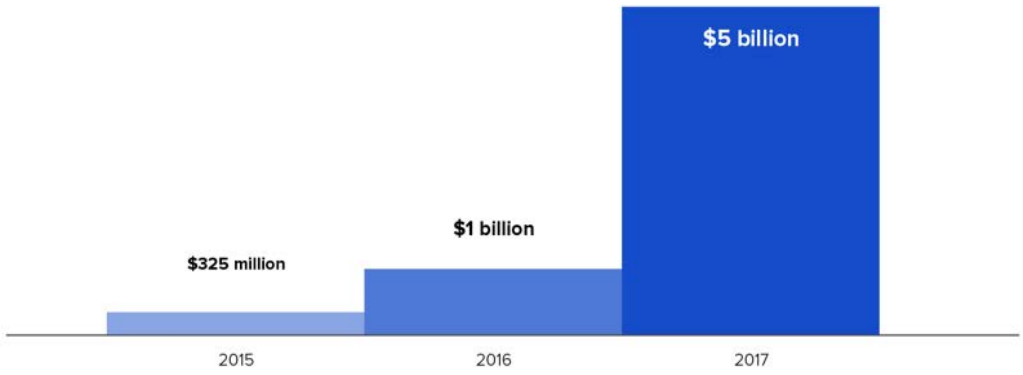
Higher educational institutions do not invest resources, time, and energy in providing the best Cybersecurity education, training, and awareness (IBM, 2019). For institutions trying, there is no regard for using the field-tested paradigm of Cybersecurity best practices or real-world scenarios. Therefore, such an outcome results in human error, leading to cyber-attacks. Attackers can bypass controls due to human errors resulting from unenforceable security policies, cybersecurity awareness, or training necessary to protect information systems, therefore, requiring human error-focused solutions. This problem will continue if cybersecurity policy deployment and training methods are not reevaluated to address gaps that could be detrimental to companies and individuals (Ahola, 2022). In recent years organized cybercriminals have changed their attention to human elements by developing advanced exploitation techniques that gain users' trust, making it easy to circumvent policies and opening avenues of attack (Khader et. al, 2021). Human factor impact in information system protection and Cybersecurity is critical due to the continuously growing and dynamically changing cyberattack methods, types, and tools (Khader et. al, 2021). Therefore, to evade cyber-attacks designed to exploit human factors, cybersecurity awareness, and policies must be developed to enable users to stay vigilant of attackers' techniques, vulnerabilities, and responsibilities. For example, Mark Evans found that in 2014, approximately 50% of the world's worst data breaches resulted from unsuspecting human error. The breach result showed an approximate 31% increase from 2013 (Evans, et. al, 2016) . The author's (Evans, et. al, 2016) work shows that half of the significant security incidents result from specific elements, including users and unintentional errors.

Furthermore, Evans (Evans, et. al, 2016) examined the complexity of human error regarding cybersecurity policies and presented a current gap in training methods and policies surrounding human error, which has led to a rise in cybersecurity attacks. Similarly, in 2017, Cybersecurity Ventures predicted (Alcon, 2016), as shown in Figure 1, that Ransomware to cost $5 billion in damages. This was rather up from $325 million in 2015.

Human error can occur at any level within the organization ranging e from the level of Executive Officers and I.T. staff to entry-level to administrative employees. For example, System Administrators can make mistakes during system configuration, application deployment, or management of security patches. Other errors can occur by implementing poor authentication procedures, including default user I.D.s and passwords. Non-technical employees can also make mistakes, including but not limited

to “using weak passwords, sharing passwords, losing devices with sensitive data on them, accessing unsafe websites, opening unsafe emails, and inadvertently sharing confidential data by sending it to the wrong email address”(Coffey, 2021).. Current literature is shifting towards a more human-centric approach to human error in cybersecurity policies. Some works” (IBM, 2014), (Nobles, 2018), (Coffey, 2021) emphasize the need to change the current policy approach, while others offer recommendations to mitigate successful attacks due to human error. Additionally, "given the number of human-enabled errors in cyber operation proves that technology alone will not eradiate human-induced mistakes." (Nobles, 2018). Such findings (Nobles, 2018), (Ahola, 2022), suggest a dire need to increase the effort in researching the human aspect of Cybersecurity in conjunction with the technological aspect to prevent continuous cyber-attacks.

Figure 1. Annual Global Ransomware Cost(Alcon, 2016)



In order to address identified problems, this research aims to address this gap in training by reviewing current security awareness training methods within higher education institutions in N.Y. States. The scope of the investigation is limited to selected higher education institutions in New York to analyze and understand the role Cybersecurity policies, awareness, and training play in informing and educating users from becoming victims or a culprit of sophisticated social engineering attacks or making unforced errors. A Triangulation research approach including quantitative, qualitative, and descriptive methods are adopted for this work. Instruments for data collection include a survey, literature review, qualitative analysis to identify research gaps, and assessments of the questionnaires. In addition, survey response from faculty members and students from one of the institutions is analyzed to establish if students and Faculty are receiving any cybersecurity training. If so, what it consists of to analyze the gaps in existing cybersecurity training and information offered? Lastly, the selected schools' Cybersecurity policies will be compared to NIST Cybersecurity Framework to evaluate the maturity of the Institution's Cybersecurity program.

The contribution of this work is in three folds. First, this work contributes literature that can be used to improve Cybersecurity awareness, training, and policies necessary to

shape an organization's cybersecurity posture concerning factors contributing to user errors and reducing cyber-attack probability. Second, this work contributes to current research by identifying many gaps in cybersecurity education, training, and awareness programs within some higher educational institutions in N.Y. States. Third, this work provides a set of recommendations necessary to impact and inform higher institutions of strategies to develop and integrate cybersecurity policies, and training into operations in order to reduce errors by users and support system functioning. Finally, we anticipate that the educational institutions within the New York area and other Institutions can leverage the recommendation to provide improved Cybersecurity organizational and situational awareness. This work is divided into section 2, a Related work review addressing previous work, findings, solutions, and gaps; section 3, Methodology; section 4, Results and discussion of findings and future work.; and section 5, Conclusion.

2. Related Work

Nixon and McGuinness (Nixon and McGuinness, 2013) reviewed the human dimension of Cybersecurity by using a framework to consider the many ways humans can positively and negatively affect the security of a system. In part, the authors (Nixon and McGuinness, 2013) focus on user training. Most often, employees are trained in the how of Cybersecurity but not the why. The context of a security procedure or process is not fully understood by the user involved in the training. The authors (Nixon and McGuinness, 2013) explain some consequences, including a user's inability to make a dependable risk assessment. Nixon and McGuinness (Nixon and McGuinness, 2013) argue that it is crucial that employees feel included in the whole organization's security program, process, training, or cultureless. The authors further argue that they can assume personal responsibility for maintaining the security of the individual component and system interaction and artifacts within the organization (Nixon and McGuinness, 2013). At the same time, because individuals rarely encounter cyber-attacks, the necessary skills are rarely, if ever, practiced after initial training"(Nixon and McGuinness, 2013).. This requirement will differ for different staff roles and responsibilities. This work is supported by Coffey's (2021) report that 56% of workers who use the Internet on their jobs receive no security training. Coffey (2021) further emphasizes that organizations that implement robust technological security procedures still regularly pay insufficient attention to human sources of vulnerability. Such a proposal has been made by several others, including Nixon and McGuinness (Nixon and McGuinness, 2013). In their work "Framing the Human Dimension in Cybersecurity," the authors (Nixon and McGuinness, 2013) emphasized the need for a periodic staff assessment as well as training that updates. This should include current threat awareness to minimize the decline of security competencies, "Over time, staff awareness of cyber threats can quickly fade, while the skills for preventing, detecting and responding to attacks can quickly become outdated."

Several research works have examined the links between user attitudes and risky Cybersecurity behaviors. In Lee Hadlington's (Hadlington, 2017) work "Human factors in

cybersecurity, examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors." The author (Hadlington, 2017) establishes the link between impulsivity and aspects of information security awareness as well as attempts to explore how individual differences in personality traits can impact a person's adherence to cybersecurity procedures (Hadlington, 2017). The impulsiveness furthers the need to study the impact of the behavior. Evans' (Evans, et. al, 2016) research found that there are metrics that can "identify current vulnerabilities faced and confirm what is an acceptable level of exposure, in order to address findings based on priority" regarding the technical security aspect (Evans, et. al, 2016. However, there is no equivalent to this mainstream mechanism for assessing and quantifying human behavior; yet some industries are addressing this by developing qualitative and quantitative techniques (Evans, et. al, 2016) These articles ultimately bring us to ask, “how can we enhance standard cybersecurity training methods for private-sector employees, in addition, to supplementing research on the element of human error in cybersecurity?”.

Notwithstanding work done by Hadlington (Hadlington, 2017) and Evans (Evans, et. al, 2016), other studies have looked at how personality traits and gender can impact online behavior. For example, Halevi et al. (Halevi et al., 2013) investigated the correlation between the Big Five personality traits and email phishing responses. The work done by Halevi et al. (Halevi et al., 2013) confirms that certain personality traits may cause higher phishing vulnerability. Furthermore, the authors (Halevi et al., 2013) demonstrate that with further research, these findings will be useful in future defenses against online attacks. Moreover, this work is supported by Holt (Holt, 2016) who focused on cybercrime through an interdisciplinary lens. Holt’s work vouches for both computer science and social science. The researchers used a holistic approach due to the multiple challenges presented by technological misuse and abuse (Holt, 2016).

The current literature has already made recommendations to optimize human performance. For example, Nobles recommends seeking human factors specialists' and behavioral analysts' expertise to develop practices addressing human error. He argues that conducting a risk assessment solely based on human factors, integrating human factor objectives into the information security strategy, and making humans-centric to the foundation of information security and cybersecurity practices (Nobles, 2018). Such recommendations place the importance of the human factor at the top of the list. This changes the prioritization of the training from the technological aspect to the human one. Nobles (Nobles, 2018) argues that although there are quality examples of ways to improve training from the information available, further research on improving our cybersecurity training is vital so that human errors are no longer prevalent reasons for system or data breaches. Furthermore, Nobles recommends that colleges and universities should offer to teach and develop human factor courses and conduct research projects on human factors. He stipulates that companies and organizations need to change what they prioritize in their training, but academic institutions also need to redirect their focus toward the human factor so that human errors can be minimized

(Nobles, 2018).

Security awareness must become integrated into academia to ensure graduates have the skills and awareness to combat cyberattacks. Work done by Khader et al. (Khader et. al, 2021) provides a conceptual cybersecurity awareness framework that guides implementing systems to improve the cybersecurity awareness of graduates in any academic institution (Khader et. al, 2021). The framework's goals are continuously improving the "development, integration, delivery, and assessment of cybersecurity knowledge into the curriculum of a university across different disciplines and majors"(Khader et. al, 2021). Using this framework would lead to better awareness among all university graduates and the future workforce in various areas of study (Khader et. al, 2021). Many other techniques have been proposed and explored (Nobles, 2018), (Ahola, 2022), (Campbell, 2017) regarding the overall impact of Cybersecurity within the human domain. Unfortunately, most of the work has been focused on tools, frameworks, and physical and technical security solutions. Our work strives, in a nutshell, to demonstrate techniques, effective alternative solutions, and counterculture approaches addressing the organization's security aspect by a focus on addressing the human aspect through administrative controls rather than the current mass solution focusing on technical and physical security.

3. Methodology

For this work, a triangulation method, including a combination of quantitative, qualitative, and descriptive, is employed in the investigation. Instruments used to collect data were a survey, literature review, and qualitative analysis to identify research gaps. This work masked the real identities of the institutions involved to minimize the possibility of exposure to vulnerabilities or gaps which bad actors can exploit. This work identified the institutions in this study as **Institutions A, B, and C**. The survey was only sent to participants (Students and Faculty) members in **Institution A with a sample size of n = 50**. Using standard statistical techniques (Pearson et. al, 2016), this sample size was determined to be significant for measuring a single population parameter. This sample size is adequate to draw scientifically significant conclusions without burdening a disproportionate number of subjects and delays. However, we had permission from I**nstitution A (the main Institution)** and the approval of the Institution's Institutional Review Board, and the participant where subjects were active willing participants. **Institutions B and C** did not include human subjects; we assessed and analyzed publicly available Cybersecurity policies and Cybersecurity awareness training information.

a. Research Design

Most of this work focuses on qualitative design, with some additional quantitative data. The first part assessed and analyzed publicly available Cybersecurity policies and Cybersecurity awareness training information about Institution A, Institution B, and Institution C. The second part is a quantitative and qualitative analysis of the survey result sent to Institution A's students and faculty members regarding their experience with cybersecurity policy and training. Finally, our study focused on user awareness and

vulnerable behaviors, effective training for users, and investigating new methods to evaluate the security posture of organizations.

b. Aim and Objective

The first objective is to assess how easy or difficult it is to find the security policies on the Institution's websites. The second objective is to assess how much the policies incorporate and address the various aspects that encompass human error to identify gaps in cybersecurity education, training, and awareness programs amongst participation selected institutions. Finally, the third objective is to use survey responses from faculty members and students at Institution A to analyze and establish if students and Faculty have cybersecurity training. The work will articulate best practices that can guide higher education institutions about Information Systems and operational weaknesses with associated threats and avenues to address Cybersecurity risk and enhance an organization's cybersecurity posture through improved and implementable cybersecurity policies and practices to reduce human errors.

c. Data Collection

This work uses data acquired from two streams. The first was survey data collected from users in Institution A. The second was Cybersecurity policies and training data available from all three institutions' websites. For the initial survey data, emails with survey questions were sent to approximately 50 users. Using a prescribed statistical approach (Person, et. al, 2016), the selected sample size is sufficient for evaluating a sole population parameter. Our second rationale for choosing the sample size was to use a sample size adequate to infer a scientifically significant culmination without the constraint of inconveniencing research participants or delays. However, we had approval from Institution A's Institutional Review Board, with the participant as active willing participants. Furthermore, for website review data collected on Cybersecurity policies and training information, both Institution B and C were unwitting participants for the Institution, considering the data is public information. Therefore, we used general Cybersecurity policies and training information on their website as part of our analysis.

Searching Institution A's website for Cybersecurity policies, we began with a search for "*Acceptable Use Policy."* Finding any information on Institution B or Institution C Acceptable Use Policy was complex. For example, after searching "*Information security policies*" in the search bar on Institution C's main website, the first link is for their computer, and the network use policy was displayed. This is because it has clear and accessible expectations of its system's users. On the other hand, institution B Information Technology Services (ITS) policies were relatively more straightforward to find than Institution A. When searching for Institution B ITS policies, we used the Google search engine and the Institution's search within its website. The searches comprised the terms and phrases "Institution B name cybersecurity policy" and "Institution B name Information Security Policy." On Institution B's website, we use more concise terms. The terms and phrases they consisted of were "I.T.," "information security policy," and "computer access." The sequence of pages to find the information security policies on

the Institution website is as such; search “ITS” on the Institution B homepage, go to “quick find,” then “About ITS,” then “policies.” On Google, this search method found the policies; search “Institution B Cybersecurity policy” on Google and choose the second result.

Institution C only has one computer and information safety policy, the “Computer and Network Use” policy. Searching for Institution “C” ITS policies was relatively easy when using Google compared to when on the Institution homepage. Using Google to search “Institution C ITS policies,” the first result was the Computer and Network Use Policy. From the homepage, searching “ITS policies” and “policies” did not result in the Computer and Network Use Policy as the first returned result. When searching “ITS policy,” the Computer and Network Use Policy was the ninth result, and when searching “policies,” a link to the “Policies and Procedures” page was the fifth result. It is possible to get to the ITS policy from the Policies and Procedures page by clicking on the “Policies and Procedures Manual,” the first link under the page's header.

When using the 2021-2022 faculty handbook for Institution C, the Computer and Network Use Policy was found under “Information Services (Computing Policies).” However, the link for the policy leads to an Institution C page with a 404-error message “the page you are looking for does not exist” (Campbell, 2017). This work is problematic because the information is not accessible, and it could deter users from searching further due to such inconvenience. Another area of concern is the Computer and Network Use Policy found on the Information Services Policies page says that its last update was 8/17/2009, and it does not include as much information as the Computer and Network Use Policy found on the Administrative Affairs policy page. Institution C's website should have the most up-to-date versions of its policies, even if they are on multiple pages.

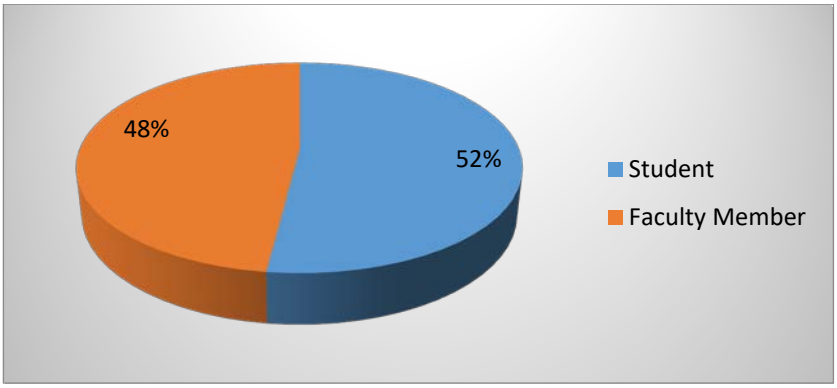
d. Data Analysis Survey

In this survey, we targeted a particular department within Institution A. The general department population is approximately 500 students and Faculty. The sample size we decided to send the survey to is approximately 50. This sample size is over 10% of the population, as most literature prescribes as an acceptable s size. Overall, the response rate was 50%. There was a total of 25 complete responses for all eight questionnaires. In a broader scheme, this response rate is higher than expected, as many previous works consider acceptable response rates ranging from 10% to 65%. For example, recent works (de Heer, et. al, 2009) examined a meta-analysis of approximately forty-five research studies which investigated the research response rate on the web survey to be lower than other types of survey. Visser et al. (Visseer et al., 2019) concluded that surveys with a nearly twenty percent response rate yield better, more acute measurements when compared to surveys with a higher response rate, such as sixty or seventy percent.

Further, Keeter et al. (Keeter et. al, 2006). evaluated outcomes from a 5-day survey leveraging g the Pew Research Center’s usual methodology, which considers a twenty-five percent response rate as acceptable found that results from a more rigorous survey

over a long period usually achieve a higher response rate of over fifty percent as compared to a short period. In 77 out of 84 comparisons, the two surveys yielded statistically indistinguishable results. Among the items that manifested significant differences across the two surveys, the differences in the proportions of people giving a particular answer ranged from 4 percentage points to 8 percentage points. Considering that our survey sent out was through a web form, we can conclude that the response rate would have been higher and sufficient for analysis. Out of the 25 responses received, thirteen of the respondents are with 13 of them being were students, and 12 were faculty members illustrating a 48% and 52% split as demonstrated in Figure 2.

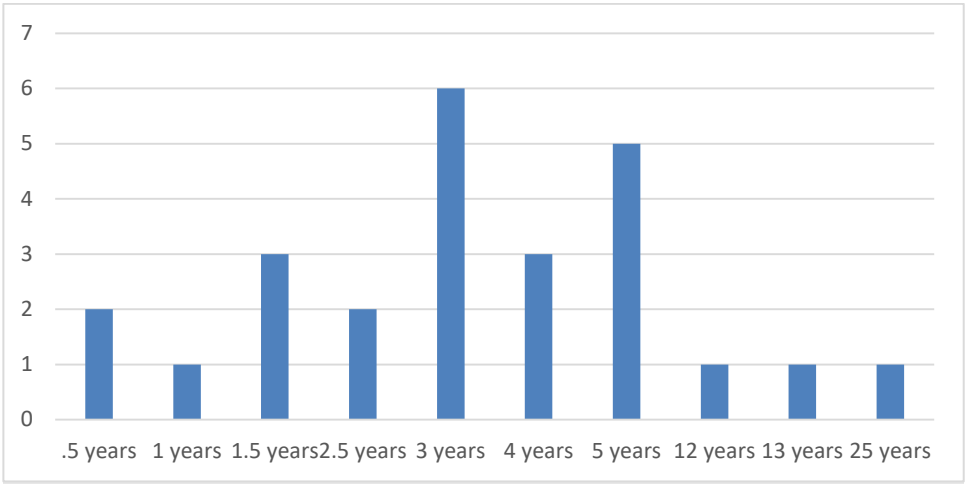
Figure 2. Percentage of student and faculty respondents



The survey questions include information on respondents' rank, position, and other specific questions relating to the duration of participant affiliation, participant cybersecurity training, participant cybersecurity awareness, and cybersecurity policies knowledge, for example, on the first question, rank, or association with the University. The results show that an almost equal number of students and Faculty are represented. We had 12 students and 13 Faculty. This demonstrated that a representative sample is vital for ensuring results are not tainted by bias. Further, such a representative sample of student and Faculty ensure that we guard against the over representing of either group since their on-campus experiences and resources may differ. This representative sample benefits our work, mainly to guide for proven accuracy as it is recognized across scientific, academic, and market research, providing credible and statistically significant results. Secondly, our representative sample provides ease and efficiency in achieving accurate and reflective results and gaining actionable insights.

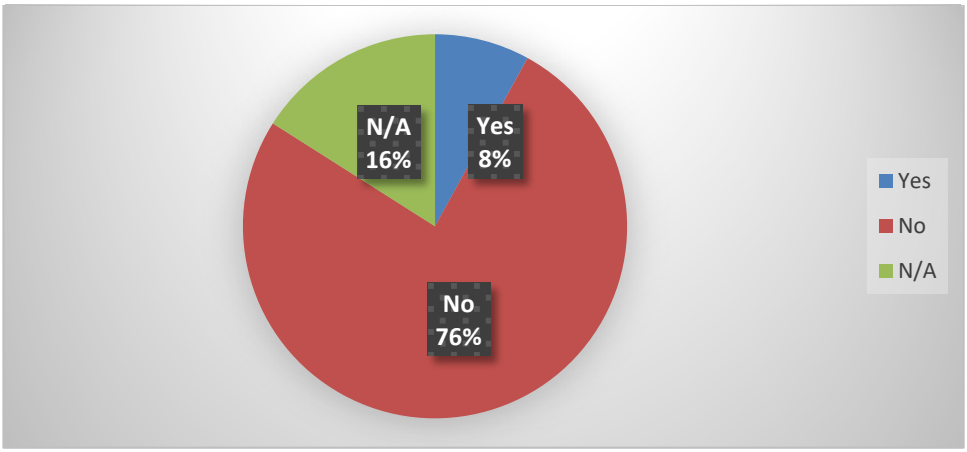
On the question, "How long have you been teaching or studying at the University"? As per our analysis of the result depicted in Figure 3, the average number of years respondents have been at UAlbany is 4.5 years, with most respondents being part of the University at Albany community for 3 years. According to the result, some respondents have only been a part of Institution A for less than a year. Other others have been here for 12, 13, or 25 years. The result demonstrates a sampled population with knowledge of old and new cybersecurity practices.

Figure 3. How long have survey participants been at the University



On the question, "Did you receive any cybersecurity training when onboarded?" Figures 4 and 5 show the data for the questions directed. Of the respondents, 8% responded 'Yes,' 76% responded 'No,' and 16% responded 'N/A.' The data shows that not enough faculty members received cybersecurity training when being onboarded. Based on the result, we can conclude that Institution A does not prioritize cybersecurity training and awareness as part of its onboarding process for both groups. The data makes it evident that members made and have not been made aware of or understand their cybersecurity resources, including policies, acceptable use, and necessary training that can prevent user errors such as phishing.

Figure 4. Did participants receive cybersecurity training during the onboarding process



For the question "if they have ever received cybersecurity training while employed at Institution A or while studying at the University," As demonstrated in Figures 5 and 6, 44% responded with 'Yes' to have received cybersecurity training whiles employed by the University, 36% responded with 'No,' and 20% responded with 'N/A.' Figure 6 shows

the percentage of respondents who have received cybersecurity training or education while studying at Institution A. This question targets students, but faculty members could also take Institution A classes. For the question, "Have you ever received Cybersecurity training or education while studying at UAlbany?" 8% responded with 'Yes,' 56% responded with 'No,' and 36% responded with 'N/A.' This question was specific to the student and demonstrated if compared to Figure 5, that more Faculty than students received cybersecurity training to some degree. However, some students could have answered 'Yes' to the question Figure 4 refers to. It is unclear if every faculty member received some training since there were 12 responses from faculty members and only 11 respondents who answered 'Yes' if they received cybersecurity training while employed by Institution A.

Figure 5. Have employees ever received cybersecurity training while employed by Institution A

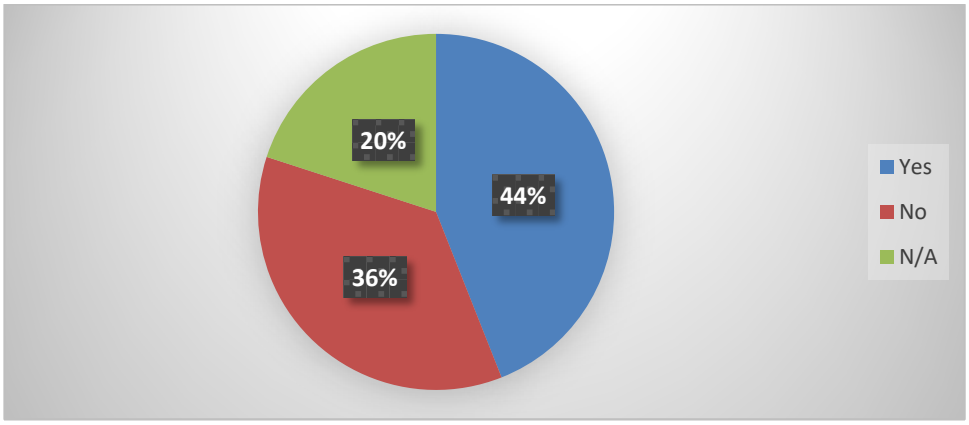
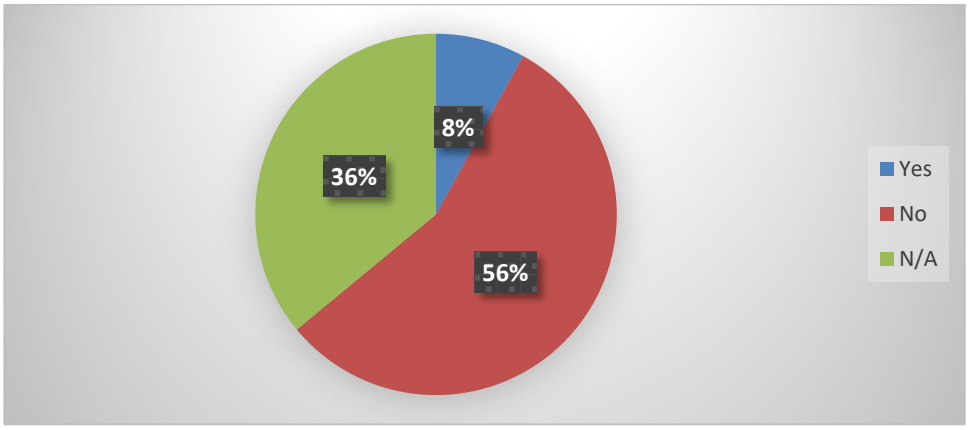


Figure 6. Have students received cybersecurity training while studying at the University



Overall, the data collected from the survey showed that Institute A students are not aware of their responsibility to protect the Institution's resources, nor have they received adequate education or training regarding Cybersecurity or information security.

e. Qualitative Analysis

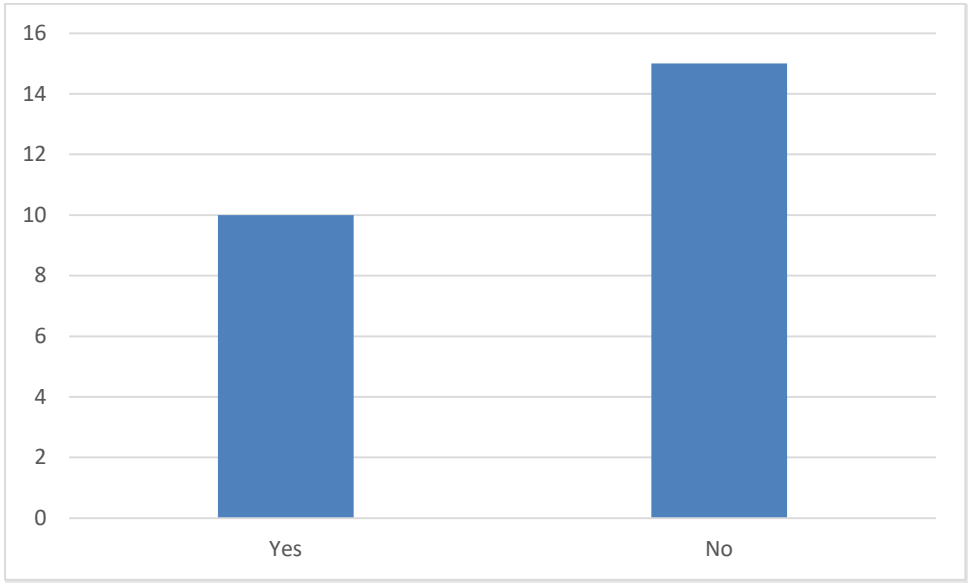
For more information on what the cybersecurity training entailed for Institution A community members, the survey asked them to describe the training in as detail as possible to assess if participants are conflicting Cybersecurity courses offered towards a degree for employee and student Cybersecurity training by the Institution. For example, one respondent took the courses CEHC 100 and CEHC 210 during their freshman and sophomore years. Although these courses are Cybersecurity courses, they are not prescribed Cybersecurity training and awareness programs develop for students and employees. The participant took the course as a degree requirement. Some faculty group respondents provide information on yearly people soft training available. A yearly Skillsoft training includes courses, videos, and compliance sessions, with one of the training sessions being about cyber security practices ("Security Awareness for End Users"). The topics that mainly seemed covered were general cyber hygiene, insider threat, and phishing.

As for one respondent, *"As Faculty, we have a mandated annual online refresher course. It is either mediocre or just plain not very good and has occasionally contained erroneous or misleading information. I am skeptical of the impact of user training in general, but I'm very skeptical of the value of this kind of training. Like much of the online mandated training, it feels more focused on box-checking compliance than on attempting to be seriously valuable."*

Other respondents had similar views saying that the course provided "rather generic information about phishing, spam, and basic cyber-hygiene practices" and covered "the different types of attacks (e.g., spear phishing) and the "do's" and "don'ts" of avoiding malware." Another respondent shared this information about the training, *"It was just the SkillSoft training, so it was a very basic, unhelpful video lesson about different kinds of cybersecurity threats and basic dos and don'ts (like don't leave your computer open and logged in unattended at a coffee shop). It covered phishing and spear-phishing but had little practical guidance in spotting these attacks."*

These unsatisfactory reviews of the Skillsoft training suggest that Skillsoft needs to review its current Security Awareness for End Users training and that UAlbany should provide end-user training with more accountability and not so "focused on box-checking." Lastly, the survey touched on how aware community members are of the University's information security policies and their responsibilities for protecting university resources. Figure 7 shows that most respondents (60%) were unaware of the policies or their responsibilities. Since the survey did not record this data, it is unclear if most respondents who answered "No" are students or Faculty. This data would be beneficial to see if more focus should be put on students, Faculty, or both.

Figure 7. Participants' awareness of the responsibility to protect University resources.



4. Discussions and Analysis

This study investigates how institutions A, B, and C in the State University of New York (SUNY) system incorporate information security and user access policies. Based on the analysis of the results, SUNY does an appropriate job of setting the standard for its universities' information security policies. Institutions A, B, and C do an acceptable job integrating the aspect of human error into their policies when evaluated against the select National Institute of Standards and Technology(NIST, 2022) subcategories. The results show how the selected Institutions' policies fared when compared to selected subcategories in NIST's Cybersecurity Framework V1.1 Core(NIST, 2022).This framework is the work resulting from "Executive Order (E.O.) 13636, Improving Critical Infrastructure Cybersecurity." It is a voluntary framework based on existing standards, guidelines, and practices for reducing cyber risks to critical infrastructure(NIST, 2022). The subcategories used to evaluate the policies were chosen based on their relevance to this research and human error. The subcategories are the Identity Management, Authentication, and Management Control (PR.AC) and Awareness and Training (PR.AT) categories. To examine the policies, they were compared to the informative references of NIST Sp 800-53 Rev. 4 because that is the source referenced in NIST's Cybersecurity Framework V1.1 Core.

The first category in which the subcategories were chosen was "Identity Management, Authentication, and Access Control." The first subcategory selected was "PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes", which establishes the necessity for a cybersecurity framework(NIST, 2022). Additionally, this subcategory is relevant to addressing human error because the policies assure that users have the correct

privileges and that the authentication method is complex enough (for example, implementing multi-factor authentication). The NIST reference AC-1, one of the informative references, states that an organization's access control policy should "address purpose, scope, roles, responsibilities, and management commitment" (NIST, 2022). Institutions A, B, and C have access control policies explaining and acknowledging the differences between accounts and who is responsible for them. The SUNY Information Security Guidelines also cover P.R.AC-1 requires that SUNY Institutions declare campus and policy standards and establish program organization and responsible authorized experts (ISO). Campus and policy standards must communicate "to appropriate members of the campus community the campus categorization and classification of sensitive information and assets" (SUNY, 2008).

For example, Institution A, Identity and Access Management Policy cover the principles for issuing electronic identifiers (PIN, Institution ID, and Net ID) and the authorities responsible for verifying identities, roles, and statuses. Establishing who is responsible for different accounts is beneficial for two reasons. First, it allows for better management because one office or group will not have to keep track of every account, just those they are accountable for. Second, it points users to a centralized location to request help regarding their accounts or other support-related issues. Furthermore, the Institution's Identity and Access Management Policy define the terms "electronic identifiers," "employee," "student," "university," and "university-related organization or organization(s)" (Albany, 2012). A policy must define its key groups so that users and managers know what group they belong to and their roles and duties. As a result, institution A's Identity and Access Management Policy successfully manage its users' identities, roles, and responsibilities regarding access to information resources.

Institution B also has a University Information Security Program, which addresses the departments responsible for information security. The Information Security Program states that the responsible groups are the Information Security Council and University designated staff, Data Stewards, Chief Information Security Officer, I.T. Security Department, Technical support, and Data Custodians. The program outlines these groups' organizational and functional responsibilities and responsibilities concerning information security (such as ensuring proper requirements, controls, and policies are being met) (Binghamton, 2022). Another ideal aspect of Institution B's University Security Program is the individual accountability covered by the category of University Data Users. It stipulates that users of university resources must protect those resources in their care and report any suspected security incident through the document process in the Security Incident Management and Response section of this policy (Binghamton, 2022). This policy effectively assigns, manages, and verifies identities and credentials for authorized users and communicates who manages certain user accounts and processes.

Institution C Computer and Network Use Policy also does a sufficient job of addressing. P.R.AC-1. Their policy separates identities and roles between students, employees, and public and guest accounts and defines who is included in each account. This is followed by the entities responsible for managing various accounts' authorization and

termination processes. Institution C Computer and Network Use Policy also discusses the management's duties. However, there is not a large difference between responsibilities for different accounts. While the Information Services (I.S.) The department manages and maintains the operation and integrity of technology systems at Institution C; all users are ultimately responsible for their accounts (NIST, 2022). The following subcategory was P.R.AC-2, which deals with physical access to assets. By complying with this subcategory, policies assure that "physical access to assets is managed and protected" (NIST, 2022). Allowing unauthorized users physical access to systems and sensitive information is another way for well-meaning users to cause harm to their organization unintentionally. Therefore, physical access is important when evaluating human error in Cybersecurity and computer use policies. All three universities address physical security; however, Institution A could go into more depth than the other two universities. The SUNY information security guidelines also address physical security by obligating universities to set up required security controls (e.g., administrative, technical, and physical) necessary to secure information systems (SUNY, 2008).

There are two controls from the NIST reference document that these policies were compared against regarding physical access, PE-2, and PE-5. PE-2 requires authorized users with facility access to the system location and the issuance credentials. PE-5 requires physical access to information system output devices to prevent unauthorized entities from gaining access. Such output devices (e.g., monitors, printers, copiers, scanners) can convert information into a humanly perceptible form (NIST, 2022]. Regarding physical access, Institution A Information Security Policy states that it will include controls (e.g. administrative, technical, and physical) appropriate to the size and complexity of the University and the sensitivity of its information. However, it does not specify what users should do or what the physical safeguards are (Albany, 2012). As for the informative references, this policy does not outline the types of individuals allowed access to facilities with sensitive information, nor does it mention how it will safeguard against unauthorized individuals accessing information system output devices.

Institution B Information Security Program policy details their physical access control mechanisms. Under the section titled "Access Control," the policy states that the University's physical control mechanisms are "commensurate with the value, sensitivity, consequences of loss or compromise, legal requirements and ease of recovery of these assets" (Binghamton, 2017). This policy better differentiates the levels of security between assets by having corresponding control measures for them. The access control policy states that it will do this by "ensuring that appropriate information security requirements for user access to automated information are defined for files, databases, and physical devices assigned to their areas of responsibility" (Binghamton, 2017). Additionally, it states which departments are responsible for this.

Furthermore, Institution B Guidelines for Data Security Policy has a section regarding controlling access to rooms and file cabinets where paper records are kept. The three points it touches on are keeping confidential information behind locked doors,

prohibiting unescorted guests in areas where sensitive information is in plain sight, and adequately disposing of privileged documents in designated recycling or shredding containers (Binghamton, 2022). While it covers simple aspects of physical access, its inclusion is nonetheless beneficial because of how easy it can be not to obey these guidelines. Institution B's policies regarding access control do an adequate job regarding PE-5 (preventing unauthorized individuals from accessing output devices). However, PE-2 does not mention having a list of authorized individuals or groups who can access the facility where the system resides.

Institution C partially addresses PE-5 in its Computer and Network Use Policy in various sections. The first section that addresses physical and account security is "Standard Security and Maintenance Practices for All Users." The maintenance practice it covers is the responsibility of users to "physically secure computers and other devices configured to access the network and log off systems containing sensitive data before they leave their workspace, even for a short time" (Nobles, 2018). This addresses PE-5 by physically restricting the availability and accessibility of information from output devices for unauthorized users. Furthermore, the section titled "Data Security and Transport of Confidential, Mission Critical, and Personally Identifiable Information" requires that physical security methods must be used at all times "to protect any removable or easily transported media containing confidential, mission-critical, or personally identifiable information" (Nobles, 2018). Again, their policy covers accessibility to information from output devices comprising sensitive information. Lastly, the Computer and Network Use Policy prohibits unauthorized access by expecting users to "log off systems, the network, and lock their offices and workspaces when they leave to secure client computers physically." Most of the responsibility for physical access is placed on the user, which is why everyday users must be made aware of their role regarding information security. Overall, Institution C Computer and Network Use Policy sufficiently manage and protects physical access to assets that address NIST's P.R.AC-2 subcategory.

In addition to the subcategory P.R.AC-2 deals with physical access, this work compares the SUNY system policies against the subcategory P.R.AC-4. P.R.AC-4 deals with access permissions, authorizations, and incorporating the principles of least privilege and separation of duties. This subcategory was included because the principle of least privilege, an information security concept where a user is given the minimum levels of access or permissions needed to perform their job functions, is important for mitigating the impact of a comprised account. When setting up and managing accounts, ensuring that users receive only the privileges necessary for their job is crucial. If an account becomes compromised, unauthorized access will be limited to only the operations that the specific user has the privilege to perform.

The SUNY Information Security Guidelines address the principle of least privilege when discussing the analysis of practices and protections. When analyzing their University's policies, it requires that the ISO, or employees of equal stature and responsibility, include these categories: "Access, Identity, Authorization" and "Minimums, Need-To-Know." The former includes "practices and protections that limit only to authorized

persons and processes the access to 'Sensitive Information. This includes 'Sensitive Systems' and limits such access only to authorized transitions and functions." The latter category encompasses "practices that keep to a minimum, based on business need, the types and instances of 'Sensitive Information used in the business processes and the persons and processes authorized to access it" (SUNY, 2016). By ensuring that SUNY universities adhere to these guidelines and categories, the SUNY guidelines comply with the NIST best practice P.R.AC-4.

Institutions A and C mention the principles their access management is based on. However, Institution B does not mention the least privilege in its policies. The NIST informational reference used for the subcategory P.R.AC-4 is AC-6. This control ensures that the organization implements the principle of least privilege, "allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks following organizational missions and business functions" (NIST, 2022). Institution "A" Identity and Access Management Policy states that "access to online services is granted based on the 'least privilege' principle"(NIST, 2022). In Institution Computer and Network Use Policy, it declares that all accounts and data access are granted or terminated on a "need-to-know basis related to the performance and fulfillment of the user's current responsibilities," which is precisely what NIST suggests for managing accounts (Nobles, 2018). Furthermore, it goes on to acknowledge that "as these responsibilities evolve, the authorization will change as appropriate" (Nobles, 2018). This requires that **Institution C** I.T. department routinely monitors account privileges, benefiting their organization by ensuring users have correct privileges over time.

Institution B's information security policies do not mention the principle of least privilege. However, their Information Security Program mentions a User Management Process established regarding access control. The University outline identifies and manages user functions to "ensure that only authorized individuals have access to University applications and information and that these users only have access to the resources required for authorized purposes" (Binghamton, 2022).. It explains the sub-processes of the User Management Process, which include granting, removing, and a periodic review of "privileged accounts" to a user. While there is no mention of implementing the principle of least privilege, they do a satisfactory job addressing P.R.AC-4 concerning access permissions and authorizations.

5. Recommendation & Conclusion.

This work investigates cybersecurity attacks attributed to failure attributed to human errors and compares different Cybersecurity education, training, and awareness in higher education institutions in N.Y. States. The scope of the investigation to limited to selected higher education institutions and the SUNY system and provide analysis and understanding of the role Cybersecurity policies, awareness, and training play in informing and educating users about making an error that can turn them into victims or a culprit of sophisticated social engineering attack or make unforced errors. Our study

focused on user awareness and vulnerable behaviors, effective training for users, and investigating new methods to measure and evaluate the security posture of organizations. The outcomes of this study indicated that all the Institutions involved have Cybersecurity use policies. The policies sufficiently meet NIST's Cybersecurity FrameworkV1.1 Core subcategories selected, but based on the empirical information from the survey from Institution A proves that the survey respondent indicates that many participants do not accurately receive any Cybersecurity awareness training or know where the policies documents are located. As a result, we can conclude that although the institutions meet NIST policies there Originally, the current policies deployment will not address human error. As a result of the findings in this work, the focus is on two areas of recommendation for the institutions: policy and training. Policies are essential to organizations because they provide a system for everyday operations. By having high-quality, relevant, well-disseminated, and well-understood policies, universities can better protect themselves against cyber-attacks stemming from human error. The other portion of recommendations, training, is essential because the universities' policies call for user training.

Regarding the policies reviewed, the information security policies and computer access policies established by the SUNY system for affected Institutions, such as the ones once studied, do a satisfactory job addressing NIST's subcategories in NIST Cybersecurity Framework. There are many more subcategories that their policies can be evaluated against, so it would be ideal for each Institution to review the remaining subcategories relevant to the University's needs. The policies can have a human-centric or a more technological approach. The human-centric policies should be geared towards training and behaviors, while technological policies should complement the training and enforce what is being taught.

The SUNY Information Security Policy requires that SUNY institutions provide annual training to "all individuals who access State University information assets and systems" (NIST, 2022). From this research, we can confirm that most of the study participants implementing yearly training for Faculty are unaware of such training, and some complain that it may not be adequate. Also, effectiveness is uncertain due to negative reviews. One way to better secure SUNY information and assets is to implement more specific requirements for the local campus policies and investigate how beneficial the policies are.

Some examples of human-centric safeguards that can be made into policies and procedures range from positive reinforcements for good behaviors and basic awareness campaigns to the threat of termination for bad behaviors. If there is no incentive to comply with the procedures and retain the information from the training, then the number of attacks deriving from human error will continue to rise. More specifically, some policies could call for the creation of security checklists. This makes policies and procedures high-profile, creating explicit disciplinary measures for lax security practices and raising the threat of litigation as measures that can encourage or coerce people into better security practices" (Coffey, 2021). Coffey (2016) also suggests awareness

campaigns that elevate the general knowledge of information security and safety.

As for training, some ways to improve security awareness are modeling and simulations, gamification, and periodic review of best practices for end-users. Niazi (Niazi, 2019) explains that modeling and simulations can improve research by developing and implementing new techniques, tools, and strategies. Furthermore, modeling and simulation can be used when real experimentation is not convenient, dangerous, or not cost-effective (Niazi, 2019) . Gamification techniques in training would help keep the end-user motivated and engaged and enhance the learning experience by making lessons more enjoyable and interactive and allowing users to see real-world applications. Gamification in training that uses rewards and positive reinforcement would raise end-user interest and participation and ultimately elevate the effectiveness of the training.

Another aspect of security awareness is the Institution's culture. SUNY institutions should build an institution-wide culture and participation where decision-making and application of Cybersecurity best practices develop into daily pursuits for end-users at all levels (Khader, et. al., 2021). Implementing a culture of cyber awareness helps users learn to understand their role in keeping their information safe. Changing a culture is an arduous process. It is also suggested that upper-level management communicate the value and purpose of cybersecurity education before implementing training and upholding the practices they enforce on the end users. Understanding the value and purpose of the training makes the learning more meaningful and makes the users more likely to pay attention because they know what is at stake.

In conclusion, SUNY institutions have policies that show they know the importance of information security and human error. However, the policies' implementation and the end-user's awareness must be reviewed in more depth to understand how functional and worthwhile the policies are full. Additionally, the training mentioned in the policies should receive more attention because it is crucial to mitigating cyber-attacks stemming from human error. Finally, the reviewed policies fare well against the part of the NIST framework utilized in this research. However, due to the limited subcategories assessed, these policies would benefit from further examination of a more in-depth comparison of the entire NIST framework.

Furthermore, surveys tailored to a university's Faculty or students would yield data that indicates that group's security awareness. The human factor is becoming increasingly important for an organization's cyber defense because human error is a primary reason for security breaches. For future cybersecurity research, there must be a shift from the technical aspect to the human aspect to prevent the frequent occurrence of successful cyber-attacks.

References

Ahola, M. (2022) The role of human error in successful Cybersecurity breaches, Usecure. [Online Document], 2022. Available: Usecure.com Online https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches [Accessed: January 30, 2022]

Alcon J. (2016) 13% of the higher education sector has been infected with ransomware, Cyber Risk Analytics & Security Ratings, 13-Oct-2016. [Online]. Available: https://www.bitsighttech.com/blog/higher-education-infected-with-ransomware. [Accessed: 15-Aug-2022].

Barati, M. & Yankson, B. (2022) Predicting the Occurrence of a Data Breach.International Journal of Information Management Data Insights, Volume 2, Issue 2, ISSN 2667-0968, https://doi.org/10.1016/j.jjimei.2022.100128.

Blackborrow, J., Christakis, S. (2019) Complexity In Cybersecurity Report 2019 - How Reducing Complexity Leads To Better Security Outcomes. Tech. Rep. May, Forrester's Security & Risk research group. 2019.

Binghamton University. (2022.). *Binghamton University computer and network policy (acceptable use).* Binghamton University. Binghamton: N.Y. [Online Document], 2022. Available:]. https://www.binghamton.edu/its/about/governance/policies/comp-net-usage-acceptable-use.html [Accessed: March 27, 2022]

Coffey, J. (2021) Ameliorating Sources of Human Error in CyberSecurity: Technological and Human-Centered Approaches. Journal of Systemics, Cybernetics, and Informatics. [Online Document], 2021. Available: iiis.org Online https://www.iiis.org/CDs2017/CD2017Spring/papers/ZA253LY.pdf. [Accessed: August 27, 2022].

Campbell, S. (2017) Cybersecurity in higher education: Problems and solutions, Toptal Insights Blog, 22-Dec-2017. [Online]. Available: https://www.toptal.com/insights/innovation/cybersecurity-in-higher-education. [Accessed: 05-Jul-2022].

Demeyer, S. (2011),Research methods in computer science. 2011 27th IEEE International Conference on Software Maintenance (ICSM), Williamsburg, VI, 2011, pp. 600-600. doi: 10.1109/ICSM.2011.6080841.

D'agostino, S. (2022) Ransomware Attacks Against Higher Ed Increase. insidehighered.com [Online Document], 2022. Available: insidehighered.com Online https://www.insidehighered.com/news/2022/07/22/ransomware-attacks-against-higher-ed-increase [Accessed: March 15, 2022].

de Heer, W, de Leeuw, E.D, Dillman, D.A, Diment, K. Dommeyer,C.J, Edwards, P., Fox, G. Fraze, S. Fricker, S. , Fricker, R.D., Galesic, M. and Goritz, A. S, (2009) Factors affecting response rates of the web survey: A systematic review Computers in Human Behavior, 24-Nov-2009. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0747563209001708. [Accessed: 05-Dec-2022].

Evans, M., Maglaras, L.A., He, Y., and Janicke, H. (2016) Human behavior as an aspect of cybersecurity assurance, Security and Communication Networks, vol. 9, no. 17, pp. 4667–4679, 2016. https://doi.org/10.1002/sec.1657

Hadlington, L. .(2017) Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors, Heliyon, vol. 3, no. 7, 2017. https://doi.org/10.1016/j.heliyon.2017.e00346

Halevi, T. Lewis, J & Memon, N. (2013) Phishing, Personality Traits, and Facebook.http://arxiv.org/abs/1301.7643.

Holt, T. (2016) Cybercrime through an interdisciplinary lens. Routledge Taylor & Francis Group. 2016. https://doi.org/10.4324/9781315618456.

IBM. (2014) IBM Security Services 2014 Cyber Security Intelligence Index. IBM Corporation.

[Online Document], 2014. Available: IBM.com Online https://www.ibm.com/downloads/cas/ZBZLY7KL [Accessed: March 5, 2022]

IBM. (2019) Cost of a Data Breach Report 2019, IBM Security. [Online Document], 2019. Available: IBM.com Online [Accessed: August 5, 2022]

IBM, (2022) IBM Report: Cost of a Data Breach Hits Record High During Pandemic. 2022. Available: newsroom Online https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic [Accessed: August 15, 2022] [Accessed: Aug. 23, 2022]

James, A., Winnefeld S., Kirchhoff, C., &Upton, D. (2015) Cybersecurity's Human Factor: Lessons from the Pentagon. [Online Document], 2022. Available: HBR Online https://hbr.org/2015/09/cybersecuritys-human-factor-lessons-from-the-pentagon [Accessed: July 23, 2022]

Keierleber, M. (2022) L.A. schools and the mystery of missing ransom note, IBM Corporation. [Online Document], 2022. Available: IBM.com Online https://www.the74million.org/article/la-schools-and-the-mystery-of-the-missing-ransom-note/ [Accessed: March 5, 2022]

Khader, M., Karam, M., and Fares, H. (2021) Cybersecurity Awareness Framework for Academia, *information*, vol. 12, no. 10, p. 417, 2021. https://doi.org/10.3390/info12100417.

Keeter, S., Kennedy, C., Dimock, M., Best, J. Craighill, P.(2006) *Public Opinion Quarterly*, Volume 70, Issue 5, 2006, Pages 759–779, https://doi.org/10.1093/poq/nfl035

Marcelino, A. (2022) Intel Selects Check Point Quantum IoT Protect for RISC-V Platform. InfoSecurity. [Online Document], 2022. Available: InfoSecurity.com https://www.infosecurity-magazine.com/search/?q=Check%20Point [Accessed: April 5, 2022].

NIST. (2022) Security and privacy controls for federal information systems and organizations. (U.S. Department of Commerce, Washington, D.C.), NIST Special Publication 800-53, Rev 4., [Online Document], 2022. Available: http://dx.doi.org/10.6028/NIST.SP.800-53r4 [Accessed: March 27, 2022].

Nixon J., and McGuinness, B., (2013) Framing the human dimension in cybersecurity, *ICST Transactions on Security and Safety*, vol. 1, no. 2, 2013. https://doi.org/10.4108/trans.sesa.01-06.2013.e

Nobles, C. (2018) Botching Human Factors in Cybersecurity in Business Organizations. Holistica. 9. 71-88. 10.2478/hjbpa-2018-0024.

Niazi, M. A. (2019) Modeling and simulation of Complex Communication Networks. Stevenage, Herts, United Kingdom: The Institution of Engineering and Technology, 2019.

Person, T., and Holt, T. (2016) Cybercrime through an interdisciplinary lens, Taylor & Francis, 21-Dec-2016. [Online]. Available: https://www.taylorfrancis.com/books/edit/10.4324/9781315618456/cybercrime-interdisciplinary-lens-thomas-holt. [Accessed: 05-Dec-2022].

Privacy Rights Clearinghouse (2021), Data Breaches, Available: https://privacyrights.org/data-breaches [Accessed May 05, 2021

The State University of New York. (2022) System-wide print resource use. (SUNY Document No. 6902). SUNY. New York: The NY [Online Document], 2022. Available: https://www.suny.edu/sunypp/documents.cfm?doc_id=891 [Accessed: March 27, 2022].

The State University of New York. (2016). *Information security policy*. (SUNY Document No. 6900). SUNY. New York: N.Y. [Online Document], 2022. Available: https://www.suny.edu/sunypp/documents.cfm?doc_id=848 [Accessed: March 27, 2022].

The State University of New York at Canton. (2022), Faculty Handbook, SUNY Canton. Canton: N.Y. [Online Document], 2022. Available: Canton.edu Online https://www.canton.edu/media/pdf/faculty_handbook.pdf [Accessed: January 17, 2022].

The State University of New York. (2008). *Information security guidelines: Campus programs & preserving confidentiality*. (SUNY Document No. 6608). SUNY. New York: N.Y.

University at Albany. (2012). *Identity and access management*. (Adopted Policy No. 5.1). University at Albany. Albany: N.Y. [Online Document], 2022. Available:. https://www.albany.edu/risk-management-compliance/policy/identity-and-access-management [Accessed: March 27, 2022]

Visser, P. Krosnick, J. Marquette, J. & Curtin M. (2019) Mail surveys for election forecasting? An evaluation of the Columbus Dispatch poll. *Public Opinion Quarterly, 60*(2), 181–227. 2019

Webster, M. (2022) Human error definition & meaning, Merriam-Webster, 2022. Available: Merriam-Webster Online https://www.merriam-webster.com/dictionary/human%20error [Accessed: March 27, 2022].